

MENU

SEARCH

INDEX

DETAIL

JAPANESE

LEGAL  
STATUS

1 / 1

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140239

(43)Date of publication of application : 17.05.2002

(51)Int.Cl. G06F 13/00

G06F 12/00

G06F 15/00

(21)Application number : 2001-236093

(71)Applicant : MIZUNO MASAHIRO

(22)Date of filing : 03.08.2001

(72)Inventor : MIZUNO MASAHIRO  
SUZUKI KAZUNARI

(30)Priority

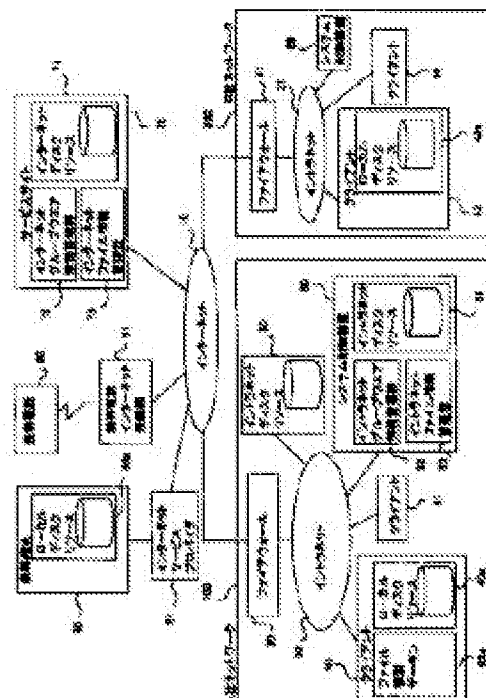
Priority number : 2000247446  
2000 227025Priority date : 17.08.2000  
23.08.2000Priority country : JP  
US

## (54) INFORMATION MANAGEMENT SYSTEM, INFORMATION MANAGEMENT METHOD AND SYSTEM CONTROLLER

(57)Abstract:

**PROBLEM TO BE SOLVED:** To construct an information management system allowing a seamless access to information from the inside and outside of an intranet where conventionally information transmission between the Internet and the intranet has not been able to pass a system having high level security provided with a fire wall or the like.

**SOLUTION:** A system controller 60 for managing groupware information and files is provided on the intranet 30. A service site 70 is provided on the Internet 10. File duplicating daemons 63c are provided in each client 40 and 41. The file duplicating daemons 63c transfer files of data on the client 40 to disk resources 50, 61, and 71 on the intranet or the Internet in coordination with the system controller 60. The system controller 60 synchronizes the groupware information in coordination with the service site 70. In such manner, information can be seamlessly accessed from inside and outside the intranet.



(19)日本国特許庁 ( J P )

(12) 公 開 特 許 公 報 ( A )

(11)特許出願公開番号

特開2002-140239

( P2002-140239A )

(43)公開日 平成14年 5 月17日 (2002. 5. 17)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード*(参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 2
12/00	5 3 3	12/00	5 3 3 J 5 B 0 8 5
	5 4 6		5 4 6 A 5 B 0 8 9
15/00	3 1 0	15/00	3 1 0 U

審査請求 未請求 請求項の数9 ○L (全 19 頁)

(21)出願番号 特願2001-236093(P2001-236093)

(22)出願日 平成13年 8 月 3 日(2001. 8. 3)

(31)優先権主張番号 6 0 / 2 2 7 0 2 5

(32)優先日 平成12年 8 月23日(2000. 8. 23)

(33)優先権主張国 米国 ( U S )

(31)優先権主張番号 特願2000-247446(P2000-247446)

(32)優先日 平成12年 8 月17日(2000. 8. 17)

(33)優先権主張国 日本 ( J P )

(71)出願人 500388442

水野 正博

アメリカ合衆国 95008 カルフォルニア

州 キャンベル ソプラトドライブ 381

(72)発明者 水野 正博

アメリカ合衆国 95008 カルフォルニア

州 キャンベル ソプラトドライブ 381

(72)発明者 鈴木 一成

アメリカ合衆国 94610 カルフォルニア

州 オークランド リーストリート 264

スイート102

(74)代理人 100099461

弁理士 溝井 章司

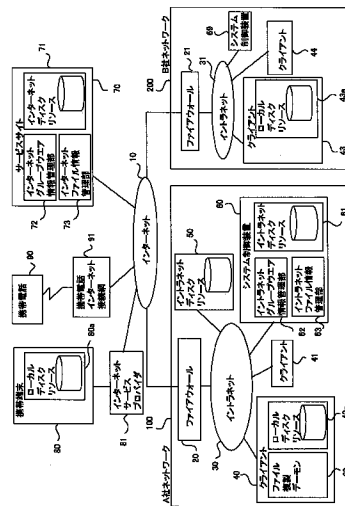
最終頁に続く

(54)【発明の名称】 情報管理システム及び情報管理方法及びシステム制御装置

(57)【要約】

【課題】 イン트라ネットとインターネット間の情報伝達はファイアウォール等を設けたハイレベルのセキュリティを有するシステムを通過できず、イントラネットの内外からシームレスに情報をアクセスできる情報管理システムを構築できなかった。

【解決手段】 イン트라ネット30上にグループウェア情報とファイル管理のためのシステム制御装置60を備え、インターネット10上にはサービスサイト70を備え、各クライアント40、41にファイル複製デモン63cを備えた。ファイル複製デモン63cは、システム制御装置60と協調してクライアント40上のデータをイントラネット上あるいはインターネット上のディスクリソース50、61、71にファイル転送する。また、システム制御装置60は、サービスサイト70と協調してグループウェア情報の同期を取る。こうして、イントラネットの内外からシームレスに情報をアクセスすることができる。



【特許請求の範囲】

【請求項1】 アクセス端末を接続するインターネットと、

ファイアウォールを介してインターネットに接続され、クライアントを接続したイントラネットとを有するネットワークシステムの情報管理システムにおいて、イントラネットに接続され、イントラネットに接続されたクライアントによりアクセスされるデータをマスターデータとして記憶するとともに、マスターデータをイントラネットからインターネットに対して転送するシステム制御装置と、インターネットに接続され、システム制御装置から転送されたデータを受信して受信したデータをマスターデータの複製データとして記憶し、記憶した複製データをインターネットに接続されるアクセス端末からアクセスさせるサービスサイトとを備えたことを特徴とする情報管理システム。

【請求項2】 上記システム制御装置は、クライアントによるマスターデータの更新を監視し、サービスサイトの複製データに対してマスターデータと同一の更新を行うとともに、アクセス端末による複製データの更新を監視し、システム制御装置のマスターデータに対して複製データと同一の更新を行う情報更新デモンを備えたことを特徴とする請求項1記載の情報管理システム。

【請求項3】 上記システム制御装置は、マスターデータとして複数の個人情報を記憶し、複数の個人情報からグループ情報を生成するイントラネットグループウェア情報管理部を備え、上記サービスサイトは、上記複数の個人情報を受信して複製データとして記憶し、複数の個人情報からグループ情報を生成するインターネットグループウェア情報管理部を備えたことを特徴とする請求項1記載の情報管理システム。

【請求項4】 上記情報管理システムは、更に、クライアントにおいて動作し、クライアントからサービスサイトへデータを転送するファイル複製デモンを有し、上記システム制御装置は、複製データをサービスサイトに転送する条件をファイル複製ポリシーとして記憶し、ファイル複製ポリシーに基づいてクライアントが所有しているファイルをサービスサイトに転送するようにファイル複製デモンに指示することを特徴とする請求項1記載の情報管理システム。

【請求項5】 上記システム制御装置は、アクセス端末又はクライアントからサービスサイトの複製データを選択させて、選択されたサービスサイトの複製データをアクセス端末又はクライアントへダウンロードするファイル制御部を備えたことを特徴とする請求項4記載の情報管理システム。

【請求項6】 アクセス端末を接続するインターネットと、

ファイアウォールを介してインターネットに接続され、クライアントを接続したイントラネットとを有するネットワークシステムにおける情報管理方法において、イントラネットに接続されたクライアントによりアクセスされるデータをマスターデータとして記憶するとともに、マスターデータをイントラネットからインターネットに対して転送するシステム制御工程と、システム制御工程により転送されたデータを受信して受信したデータをマスターデータの複製データとして記憶し、記憶した複製データをインターネットに接続されるアクセス端末からアクセスさせるサービスサイト工程とを備えたことを特徴とする情報管理方法。

【請求項7】 アクセス端末を接続するインターネットと、

インターネットに接続され、データを記憶し、記憶したデータをインターネットに接続されるアクセス端末からアクセスさせるサービスサイトとファイアウォールを介してインターネットに接続され、クライアントを接続したイントラネットとを有するネットワークシステムのイントラネットに接続されたシステム制御装置において、イントラネットに接続されたクライアントによりアクセスされるデータをマスターデータとして記憶する記憶部と、マスターデータをイントラネットからインターネットのサービスサイトに対して転送して、複製データとしてサービスサイトに記憶させる情報管理部と、クライアントによるマスターデータの更新を監視し、サービスサイトの複製データに対してマスターデータと同一の更新を行うとともに、アクセス端末による複製データの更新を監視し、システム制御装置のマスターデータに対して複製データと同一の更新を行う情報更新デモンとを備えたことを特徴とするシステム制御装置。

【請求項8】 上記サービスサイトは、アクセス端末からデータアクセス要求がある場合に、データアクセス要求のあったマスターデータをシステム制御装置から複製データとして複製してきて一時的に記憶するとともに、アクセス端末からのデータアクセス要求の消滅により複製データを消去することを特徴とする請求項1記載の情報管理システム。

【請求項9】 上記サービスサイトは、アクセス端末が生成したマスターデータに対する入出力コマンドをシステム制御装置に対して転送し、システム制御装置は、サービスサイトから転送された入出力コマンドをマスターデータに対して実行することを特徴とする請求項1記載の情報管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、グループウェア機能とファイル共有機能を有するイントラネットとファイアウォールを介して接続してなるインターネット等エク

ストラネット構成において、特にイントラネットのセキュリティ性能を損なうことなく、それぞれのデータの整合性管理とデータの転送を効率的に行うのに好適な情報管理システムに関するものである。

【0002】

【従来の技術】特定の企業間で秘匿性の高い情報を安全に共有するには、不正アクセスを防止するセキュリティシステムを構築することが不可欠である。例えば、イントラネット内に不正に外部からアクセスされることを防ぐために、ファイアウォールと呼ばれるゲートウェイを各イントラネットの入り口に配置している。

【0003】しかし、このような構成では、各企業のそれぞれのイントラネット内にあるグループウェア上の情報や共有したいファイルの参照がファイアウォールによって阻止される。このような問題に対処するために、従来は、図9に示す技術が用いられている。

【0004】図9は、イントラネット上のデータを外部からアクセスする場合の従来のシステムを示すブロック図である。図9において、10はインターネット、100はA社ネットワーク上のイントラネット、20はファイアウォールである。同様に、31はB社ネットワーク上のイントラネット、21はファイアウォールで各社のイントラネットを外部からの進入から保護している。40～44はクライアントである。

【0005】しかし、このような場合、A社、B社間の情報のやりとり、ファイルのやり取りをインターネット10を通じて行おうとしてもファイアウォール20又は21に阻止される。このような場合、両者は、VPN（仮想私設網）接続を行っている。A社ネットワーク100上にVPNサーバ102、B社ネットワーク上にA社のVPNサーバと互換性のある別のVPNサーバ201を設置して転送するデータを暗号化しVPNトンネル11を経由してデータを転送することによってセキュリティを確保している。

【0006】更に、ファイアウォール20にRAS（リモートアクセスサーバ）101を設け、そこに接続されているモデム103を介して外部の携帯端末80からダイヤルアップして情報やファイルを参照することも行われている。このような構成により、ファイアウォールを経由せずに、A社ネットワーク100のデータをアクセスできる。

【0007】また、外部のASP（アプリケーションサービスプロバイダ）390に業務をアウトソーシングし、A社、B社あるいは外部から共有したい情報、ファイルを全てASP390上のディスクリソース391上に格納、管理し使用参照する方法も行われている。このような構成によってインターネットを通じてどこからでも情報、ファイルを参照することができる。

【0008】また、特開平11-219326「電子ファイル管理システム」や、特開2000-148611

「イントラネットとデータベースサーバ及びそのデータ転送方法」に見られるように、情報やファイルを、例えば、電子メールの形に変換してイントラネット間の情報転送を行う方法等が考案されている。

【0009】しかしながら、このような方法では、まず情報を暗号化するための装置を、情報を参照する場合全てに用意する必要が発生し、コストがかかり、更に、互換性の問題が発生する。また、ファイアウォールを経由しない経路を作る場合は、セキュリティが十分確保できない。更に、データを外部に置く場合は、外部記憶媒体へのアクセスに時間がかかり、また、ユーザからの負荷が集中するためにシステム自身の性能が悪化することがある。また、各種端末からのログインの手順が異なり使用方法が煩雑になり、更に、情報を外部に置くために秘匿性が守れない等の問題が発生し、当該シームレスなアクセスを実現化するに至っていない。

【0010】なお、企業内ネットワーク、即ち、イントラネット30を保護するためにインターネット10との間に設けられたファイアウォール20は、メール受信用にpop3プロトコル（ポート番号110）、メール送信用にsmtpプロトコル（ポート番号25）、ファイル転送用のftpプロトコル（ポート番号21）又はWeb情報用のhttpプロトコル（ポート番号80）を利用して、なおかつ、メール以外のデータのアクセスは、イントラネットの内側から外側へのみを可能にしている。

【0011】

【発明が解決しようとする課題】従来の技術では、企業内で使用している情報、ファイルがファイアウォール等を設けたハイレベルなセキュリティを有するネットワークを通過できない。

【0012】本発明の目的は、現在使用されているセキュリティ技術を使用しつつも、シームレスなアクセスを可能とする情報管理システムを得るものである。

【0013】

【課題を解決するための手段】この発明に係わる情報管理システムの好適な実施の形態は、ファイアウォールにてセキュアされたイントラネットと、このファイアウォールを介して当該イントラネットと通信を行うことができるインターネットとを有するネットワークシステムにおいて、イントラネット上に所属する各メンバーに帰属するスケジュール等の個人情報とそのメンバが扱っているファイルを、マスタデータとして管理するシステム制御装置を備えるものである。

【0014】この発明に係わる情報管理システムの好適な実施の形態は、イントラネットから利用できるディスクリソースと、そのディスクリソース上にも上記イントラネット上の個人情報とファイルとを複製データとして格納する機能とを備えるサービスサイトをインターネット上に備えるものである。

【0015】この発明に係る情報管理システムの好適な実施の形態は、上記システム制御装置から上記サービスサイト上の個人情報と上記システム制御装置上の個人情報との両方の個人情報の変更を監視し、上記サービスサイト上の個人情報と上記システム制御装置上の個人情報を同一であるように上記サービスサイト上の個人情報と上記システム制御装置上の個人情報を操作する個人情報更新デモンを備えるものである。

【0016】この発明に係る情報管理システムの好適な実施の形態は、イントラネット上のクライアント上に、上記システム制御装置と連携を取りながら、クライアント上のマスタデータをイントラネットディスクリソース又は上記サービスサイトディスクリソースにマスタデータの複製データを転送するファイル複製デモンを備えるものである。

【0017】この発明に係る情報管理システムの好適な実施の形態は、上記ファイル複製デモンがマスタデータの複製データを生成するタイミングをファイル複製ポリシーにより設定可能である。更に、複製データの生成時には、ファイル名を変更し、ファイルを格納した時刻、格納を指示したクライアント名等のプロパティ情報を付加して転送するプロパティ付加部を備えるものである。

【0018】この発明に係る情報管理システムの好適な実施の形態は、イントラネットのクライアントからWWWブラウザで上記システム制御装置をアクセスすることによって、上記ファイル複製デモンがイントラネットディスクリソースに格納した複製データを参照し、クライアントへダウンロードするイントラネットファイル情報管理部を備えるものである。

【0019】この発明に係る情報管理システムの好適な実施の形態は、インターネットのアクセス端末からWWWブラウザで上記サービスサイトをアクセスすることによって、上記ファイル複製デモンがイントラネットから転送したインターネット上のディスクリソースに格納した複製データを参照し、アクセス端末へダウンロードするインターネットファイル情報管理部を備えるものである。

【0020】この発明に係る情報管理システムの好適な実施の形態は、上記個人情報を利用してメンバーが所属するグループのグループ情報を上記システム制御装置で生成するイントラネットグループ情報生成部と、同一のグループ情報を上記サービスサイトで生成するインターネットグループ情報生成部とを備えるものである。

【0021】この発明に係る情報管理システムの好適な実施の形態は、上記サービスサイト上の情報を、上記インターネット上に接続される各種のアクセス端末（クライアント、サービスプロバイダ経由の自宅のパソコン、携帯端末、携帯電話等）から、クライアントがユーザに提供しているユーザインタフェースと同一あるいは

類似したユーザインタフェースで、かつ、ユーザがクライアントに対して入力するパスワードと同一のパスワードでアクセス可能な機能を備えるものである。

【0022】上記サービスサイトは、アクセス端末からデータアクセス要求がある場合に、データアクセス要求のあったマスタデータをシステム制御装置から複製データとして複製してきて一時的に記憶するとともに、アクセス端末からのデータアクセス要求の消滅により複製データを消去することを特徴とする。

【0023】上記サービスサイトは、アクセス端末が生成したマスタデータに対する入出力コマンドをシステム制御装置に対して転送し、システム制御装置は、サービスサイトから転送された入出力コマンドをマスタデータに対して実行することを特徴とする。

【0024】

【発明の実施の形態】実施の形態1. 以下、本発明の実施の形態を、図面により詳細に説明する。図1は、本発明によるイントラネットと他のネットワークとの接続を示すブロック図である。図1において、10はインターネット、100はA社ネットワーク、また、200はB社ネットワークである。80はノートパソコンや自宅のパソコンを含めた携帯端末、81はそれら携帯端末80を電話網経由でインターネット10に接続するためのインターネットサービスプロバイダ、90は携帯電話、91はその携帯電話をインターネット10に接続するための携帯電話インターネット接続網である。A社ネットワーク100とB社ネットワーク200、更に、携帯端末80、携帯電話90はインターネット10を介して互いに接続されエクストラネットを構成している。

【0025】A社ネットワーク100において、20はファイアウォール、30はイントラネット、40、41はイントラネット30に接続されるクライアントである。B社ネットワーク200において、21はファイアウォール、31はイントラネット、43、44はイントラネット31に接続されるクライアントである。それぞれのイントラネットは、ファイアウォール20又は21によって外部からの攻撃に対して備えセキュリティを確保している。

【0026】A社ネットワーク100において、50はイントラネット30上のクライアント間で共有することができるイントラネットディスクリソース、60はグループウェアとファイルを管理するシステム制御装置、61はシステム制御装置60内にあって、イントラネットディスクリソース50と同様に、各クライアントから共有できるイントラネットディスクリソース、62はイントラネット30上の各ユーザのスケジュール情報、コンタクト情報等グループウェア情報を管理するイントラネットグループウェア情報管理部、63はイントラネット30上のクライアント上のファイル情報を管理するイントラネットファイル情報管理部である。また、B社ネット

ワーク200において、69はシステム制御装置60と同じシステム制御装置である。

【0027】クライアント40において、40aはクライアント40上データを格納するローカルディスクリソースで、63cはローカルディスクリソース40aのデータをイントラネットディスクリソース50やインターネットディスクリソース71に複製を作る作業するファイル複製デモンである。

【0028】サービスサイト70において、71はインターネット上にあって、A社ネットワーク100やB社ネットワーク200、携帯端末80等からアクセスすることができるインターネットディスクリソース、72はインターネット10上でA社ネットワーク100及びB社ネットワーク200上の各ユーザのスケジュール情報、コンタクト情報等グループウェア情報を管理するインターネットグループウェア情報管理部、73はインターネット10上でA社ネットワーク100及びB社ネットワーク200上のクライアント上のファイル情報を管理するイントラネットファイル情報管理部である。

【0029】次に、グループウェア関連の各データの所在、流れを概略説明する。グループウェア情報は、システム制御装置60に管理されており、マスタデータは、イントラネットディスクリソース61に存在する。データの参照、更新等の作業は、イントラネットグループウェア情報管理部62によって行われる。同様のデータがインターネットグループウェア情報管理部72によっても管理されており、データはインターネットディスクリソース71上に存在する。

【0030】次に、ファイル関連の各データの所在、流れを概略説明する。各クライアント上のデータは、例えば、クライアント40のデータは、ローカルディスクリソース40aに存在する。ファイル複製デモン63cは、ローカルディスクリソース40aのデータを複製し圧縮して、イントラネットディスクリソース50、又はイントラネットディスクリソース61、インターネットディスクリソース71にデータの圧縮複製を転送する。イントラネットディスクリソース61に転送され記憶されたデータは、イントラネットファイル情報管理部63を経由して、クライアント41に転送することができ、クライアント41でデータを復元利用することができる。

【0031】以下、図2、図3を用いてユーザインタフェースについて説明する。図2、図3の四角枠は、画面表示を示している。300はイントラネットホームページで各ユーザの入り口である。コンテンツは物理的にはシステム制御装置60にあり、各ユーザはイントラネット300に接続された任意のクライアントからWWWブラウザ経由でアクセスできる。301は各ユーザ個人に割り当てられたイントラネット個人情報ページで、イントラネットホームページ300のログイン画面にユーザI

Dとパスワードを入力することによって、各ユーザ単位に管理されたイントラネット個人情報ページ301にアクセスすることができる。302は各ユーザ個人のグループウェア情報をアクセスするための個人情報表示画面で、掲示板や行き先表示、会議室の予約等が操作確認できる。303は各ユーザが所属しているグループのスケジュール等グループメンバ全体の情報をマージした情報を確認できる画面である。画面302、303は、イントラネットグループウェア情報管理部62により作成変更されたグループウェア情報を表示するものである。

【0032】また、304は各ユーザ個人のディスクリソースを管理するリソース管理ページで、305はクライアント上のファイルをイントラネットディスクリソース50、61やインターネットディスクリソース71にファイルを転送して複製を作るタイミングや条件を設定するポリシー設定画面、306はイントラネットディスクリソース50、61やインターネットディスクリソース71にあるファイルの複製を表示して選択し、それをクライアント上にダウンロードすることができるファイルブラウザ画面、307はファイルブラウザ画面306にて表示した各ファイルそれぞれを作成された日付、バージョン、編集したクライアントの名前等のプロパティを表示するファイルブラウザ子画面である。画面304、305、306、307は、イントラネットファイル情報管理部63が管理しているファイルやデータを表示するものである。

【0033】図2において、320はイントラネットを管理する管理者のための管理者用ページでここを経由して以下の各ページにアクセスできる。321はグループウェアに参加するメンバを登録したり、あるいは共有の情報を管理するグループウェア管理画面、322はイントラネット上の各端末やその上で動作するファイル複製デモン63cの動作状態等を管理するファイルリソース管理画面である。画面321は、イントラネットグループウェア情報管理部62が管理者にのみ提供するものである。画面322は、イントラネットファイル情報管理部63が管理者にのみ提供するものである。

【0034】図3において、更に、310はインターネット10上のサービスサイト70にありインターネット上のアクセス端末からアクセスでき、イントラネットのクライアントに入力するユーザIDとパスワードと同一のユーザIDとパスワードとを入力するサービスサイトホームページで、311はその個人情報をアクセスできるインターネット個人ページであり、イントラネット個人情報ページ301に相当する情報をインターネットアクセスできるものである。312はインターネット上の個人情報表示画面で、313はインターネット上のグループ情報表示画面である。画面312、313は、インターネットグループウェア情報管理部72により作成変更されたグループウェア情報を表示するものである。3

14はインターネット上のリソース管理画面で、316はインターネットディスクリソース71上にあるファイルの複製を表示して選択し、それをインターネット経由で接続された携帯端末80等にダウンロードすることができるファイルブラウザ画面、317はファイルブラウザ画面316にて表示した各ファイルそれぞれを作成された日付、バージョン、編集したクライアントの名前等のプロパティを表示するファイルブラウザ画面である。画面314、316、317、318は、インターネットファイル情報管理部73が管理しているファイルやデータを表示するものである。

【0035】図3において、318はサービスサイト70上において、システム制御装置60やファイル複製デモン63c等の保守情報やアップグレード情報を提供すると同時に、ファイルリソース管理ページ322と連携して動作し、各サービスの課金情報等を管理するサービスページである。画面318は、サービスサイト70が管理者にのみ提供するものである。

【0036】図2と図3において、以下の画面は、同一又は類似の表示及び同一又は類似のユーザインタフェースを持っている。画面300と画面310、画面301と画面311、画面302と画面312、画面303と画面313、画面304と画面314、画面306と画面316、画面307と画面317。こうして、ユーザは、クライアントからでもアクセス端末からでも、同一の又は類似のオペレーションで同一内容のデータにアクセスできる。

【0037】以下、図4を用いてシステム制御装置60とサービスサイト70上の個人情報とグループ情報の提示に関する詳細を説明する。61a、61b、61cはシステム制御装置60上のイントラネットディスクリソース61上にある各ユーザメンバの個人情報を示すイントラネットグループウェア個人情報である。61eはイントラネットグループウェア個人情報61a、61b、61cがマージされたものであり、各ユーザメンバが所属するグループの情報を示すイントラネットグループウェアグループ情報である。62aはイントラネットグループウェア情報管理部62内の機能であり、イントラネットグループウェアグループ情報61eを生成するイントラネットグループ情報生成部である。

【0038】71a、71b、71cはサービスサイト70上のインターネットディスクリソース71上にある各ユーザメンバの個人情報を示すインターネットグループウェア個人情報である。71eはインターネットグループウェア個人情報71a、71b、71cがマージされたものであり、各ユーザメンバが所属するグループの情報を示すインターネットグループウェアグループ情報である。72aはインターネットグループウェア情報管理部72内の機能でありインターネットグループウェアグループ情報71eを生成するインターネットグループ

情報生成部である。

【0039】イントラネット上の各ユーザは、イントラネット個人情報表示画面302を使用して個人スケジュールや行き先表示、To Do List、アドレス帳等の業務で使用している情報をアクセスし更新することができる。これらの情報は、イントラネットグループウェア個人情報61a、61b、61cに記録されているものである。303は各自の個人情報を所属するグループ単位にマージした情報を表示して、同一グループの構成員達の所在や、スケジュール等を確認するために使用するイントラネットグループ情報表示画面である。これらの情報は、イントラネットグループウェアグループ情報61eとして記録される。

【0040】一方、インターネット上の携帯端末80等のアクセス端末で情報をアクセスするユーザは、インターネット個人情報表示画面312を使用して個人スケジュールや行き先表示、To Do List、アドレス帳等の業務で使用している情報をアクセスし更新することができる。これらの情報はインターネットグループウェア個人情報71a、71b、71cに記録されているものである。313は各自の個人情報を所属するグループ単位にマージした情報を表示して、同一グループ員達の所在や、スケジュール等を確認するために使用するインターネットグループ情報表示画面である。これらの情報は、インターネットグループウェアグループ情報71eに記録されているものである。

【0041】図5において、インターネットグループウェア個人情報71aを例にとって、データ構造を示したものである。他のインターネットグループウェア個人情報71b、71c及びイントラネットグループウェア個人情報61a、61b、61cも同じデータ構造を有している。グループウェア個人情報には、各ユーザが通常のディスクリソースと使用できるデータ領域とグループウェアの個人情報が記録される。更に、個人情報表示画面を通じて各クライアントや携帯端末等から入力された内容の変更分の情報が変更差分情報として記録される。

【0042】システム制御装置60上の個人情報とサービスサイト70上における個人情報のデータ配置の詳細を説明する。図6は、サービスサイト70上にあるインターネットディスクリソース71でのデータの配置を図示したものである。イントラネット30に属する個人情報データ、例えば、71a、71b、71c等がエリア71hに配置されており、グループA71fやグループB71gを構成している。例えば、グループB71gの場合は、インターネットグループウェア個人情報71aを含むメンバ1-4で一つのグループを構成している。71eは各個人情報から作られたグループA、B等のグループ情報をインターネットグループウェアグループ情報として格納するブロックである。

【0043】イントラネット30に配置されているシス

システム制御装置60のイントラネットディスクリソース61に、イントラネットグループウェア個人情報61a、61b、61cが図6と同じ形式でデータが配置されている。イントラネット30に配置されているシステム制御装置60の個人情報は、インターネットディスクリソース71上の領域71hに配置される。同様に、イントラネット31に配置されているシステム制御装置69の個人情報は、インターネットディスクリソース71上の領域71jに配置される。このようにして、複数のイントラネットの情報が一つのサービスサイトにて管理されている。

【0044】図7を用いシステム制御装置60上の個人情報とサービスサイト70上の個人情報の同期に関する詳細を説明する。ここで、同期とは、データの同一性を意味する。即ち、同期とは、マスタデータと複製データとの一方が更新された場合、他方も更新して両者を同一内容のデータとすることをいう。図7で、上半分がサービスサイト70で扱われているデータ、下半分がシステム制御装置60で扱われているデータである。インターネットグループ情報生成部72aがインターネットグループウェア個人情報71a、71bの個人情報を使って、インターネットグループウェアグループ情報71eを生成し、同様に、イントラネットグループ情報生成部62aがイントラネットグループウェア個人情報61a、61bの個人情報を使って、イントラネットグループウェアグループ情報61eを生成する様子を示している。

【0045】インターネットグループウェア個人情報の個人情報に対する変更、例えば、スケジュール等の変更が各クライアントや携帯端末から行われた場合は、個人情報が直接変更されずに、それぞれのグループウェア個人情報の変更差分情報に変更内容が記録される。それは、イントラネット上でも同様の扱いを受ける。ここで、変更とは、グループウェア個人情報の新規生成も含むものとする。例えば、新規メンバnが追加された場合、新規メンバn用のイントラネットグループウェア個人情報61nのための記憶領域が確保され、記憶すべき内容が変更内容としてグループウェア個人情報の変更差分情報に記録される。

【0046】62dはシステム制御装置60上に存在する個人情報更新デモンであり、一定期間毎に、各個人情報の変更差分情報を監視し、なんらかのアップデートがあった場合には、システム制御装置60側の個人情報、図では、イントラネットグループウェア個人情報61bの個人情報を更新する。そして、イントラネットグループウェア個人情報、図では、61bの個人情報をサービスサイト70に転送して、インターネットグループウェア個人情報、図では、71bの個人情報に書き込む。逆に、個人情報更新デモン62dは、インターネットグループウェア個人情報71bの各個人情報の変更差分情報を監視し、なんらかのアップデートがあった場

合には、インターネットグループウェア個人情報71bの個人情報を更新する。そして、イントラネットグループウェア個人情報61bの個人情報も更新する。新規メンバの追加も、変更の方法と同様の方法で行われる。こうして、サービスサイト70上とシステム制御装置60上のグループウェア個人情報の同期を、イントラネット上のクライアントからの更新と、インターネット上の携帯端末等からの更新をお互いに競合することなく、取ることができる。

【0047】以下、図8を用いてクライアント上のデータの複製に関する詳細を説明する。ユーザは、イントラネットファイル情報管理部63が提供するポリシー設定画面305からファイル複製条件を入力する。例えば、ファイル複製条件として、図8では、複製タイミングとして、ファイルAを「毎日17時00分」に複製することを指定している。このファイル複製条件は、ファイル複製ポリシーデータ63bとしてイントラネット情報管理部63に記録される。このファイル複製ポリシーデータ63bに基づいて、ファイル複製デモン63cがローカルディスクリソース40aのデータの複製を作る。図8では、クライアント41上のデータAをスケジューラ63cがファイル複製ポリシーデータ63bの複製タイミングに設定されている時刻(17:00)に従って、データD及びデータCを複製する。又は、複製タイミングが「ファイルの更新時」となっている場合は、ファイル監視部63cがファイルの更新を検知して複製する。ここで、複製とは、ファイルAの全てのデータをコピーするのではない。ファイルAへの書き込みデータに対して日付、バージョン、クライアントマシン名といったプロパティをプロパティ付加部63ccによって追加されたデータが、イントラネットディスクリソース50上のデータB及びインターネットディスクリソース71上のデータCとして転送され複製ができる。即ち、データB、データCは、プロパティが付加された差分データである。もし、ファイルAが新規に生成された場合は、ファイルAの内容全体が差分データとなる。

【0048】プロパティ付加部63ccが付加するプロパティは、例えば、以下のものがある。ファイル名を変更した場合、変更後のファイル名。ファイルを格納した時刻。格納したファイルのバージョン。ファイルの格納を指示したクライアントマシン名。更新データ、書き込みデータに対する日付。更新データ、書き込みデータのバージョン。データの更新、書き込みを行ったクライアントマシン名。

【0049】以下、図8を用いてファイル制御部63a、73aにより提供されるクライアント40及び携帯端末80でのデータの復元に関する詳細を説明する。各ユーザメンバは、ファイルブラウザ画面306、316によって必要なファイルを選択し、更に、ファイルブラウザ子画面307、317によって選択したファイルの過去の



履歴から必要なファイルを、プロパティとして付加された日付、バージョン、クライアントマシン名等から選択してダウンロードすることができる。データB、データCは、プロパティが付加された差分データであり、この差分データを用いてクライアント40又は携帯端末80にファイルAを生成できる。或いは、これらの差分データをクライアント40又は携帯端末80のファイルAのデータとをあわせることにより、更新されたファイルAを提供することができる。図では、クライアント40がデータBを自分のローカルディスクリソースにデータDとしてダウンロードした例を示している。また、インターネットディスクリソース71上のデータCを携帯端末80上のローカルディスクリソース80aにデータEとしてダウンロードした例を示している。また、クライアント40は、データCを自分のローカルディスクリソースにデータDとしてダウンロードすることもできる。しかし、携帯端末80は、ファイアウォール20があるために、データBをローカルディスクリソース80aにデータEとしてダウンロードすることはできない。

【0050】この実施の形態は、ファイアウォールがあるために、インターネット上のサービスサイト（サーバ）にあるデータのアクセスは、イントラネット内側から外側へのみしか行えず、インターネットからイントラネットの内側に対しては、データのアクセスができないというシステムを前提として、ユーザがイントラネットにアクセスできない環境下にある時でも、イントラネットにアクセスしているのと全く同じ状態を提供するものである。イントラネットのマスターデータを複製し、インターネットに設けられたサービスサイトにファイル転送することにより、マスターデータがイントラネット内にあり、複製データがインターネット上にあるという状態を作る。そして、ユーザがイントラネットのマスターデータをアクセスできないときは、インターネットに用意された複製データをアクセスする。こうして、ユーザがイントラネットにアクセスできない環境下にある時でも、イントラネットにアクセスしているのと全く同じ状態を提供することができる。また、マスターデータの更新があったときは、イントラネット内の情報更新デモンによりインターネット上の複製データも更新される。逆に、インターネット上の複製データの更新があったときは、イントラネット内の情報更新デモンによりマスターデータも更新される。情報更新デモンは、イントラネットの内側から外側へのみのアクセスを用いてデータ更新の監視とデータ更新をする。従って、情報更新デモンは、インターネットからイントラネットの内側に対してはアクセスできないという制約があっても動作できる。また、イントラネットからインターネットへのファイル転送は、ファイル複製デモンにより行われるが、ファイル複製デモンは、イントラネットの内側から外側へのみのアクセスを用いてファイル転送を行う。従って、フ

ァイル複製デモンは、インターネットからイントラネットの内側に対してはアクセスできないという制約があっても動作できる。また、インターネットからイントラネットへのファイル転送は、クライアントからインターネットへのアクセスにより行われるので、インターネットからイントラネットの内側に対してはアクセスできないという制約があっても動作できる。また、この実施の形態では、メール送受信用プロトコルを用いなくてもよいので、メール送受信用プロトコルの制約を受けない。

【0051】なお、個人情報又はファイルは、グループウェア以外に商品データベースやメール等でもよい。ファイルの転送は、前回転送分の差分情報でもよい。また、転送時にウイルスチェック等の動作を組み合わせてもよい。インターネット上に転送されたデータを他のイントラネットから参照して、複数のイントラネット環境にあるデータベース間のデータを同期させるために使用してもよい。また、前述した各部、各デモンは、ソフトウェアプログラムで実現できる。前述した各部、各デモンがプログラムとして実現される場合、プログラムは、ディスクリソース等の記憶部に記憶され、クライアントコンピュータやシステム制御装置やサービスサイト（サーバ）コンピュータのCPUにより記憶部から読み出され実行される。また、ディスクリソースとして、磁気ディスク、光ディスク、その他のディスク装置を用いることができる。ディスクリソースではなくて、その他の不揮発性記憶装置（記憶部）を用いてもよい。

【0052】以上、この実施の形態によれば、ファイアウォールにて外部から保護されたイントラネットの環境をなんら変更することなく、必要なデータだけをインターネット上のパスワード等で保護されたサービスサイトに置き、インターネット上に接続された他ネットワーク上のクライアント、ダイヤルアップした携帯端末、携帯電話などのアクセス端末から自由に情報をアクセスできる。

【0053】例えば、A社の社員である山田氏が社内設置されたクライアント40を使用して、パスワード「XYZ」を用いてローカルディスクリソース40aのファイルをアクセスしたり、イントラネットディスクリソース61のイントラネットグループウェア個人情報61aとイントラネットグループウェアグループ情報61eとをアクセスできる場合、山田氏が出張先のホテルからノートブックパソコン等の携帯端末80から同一のパスワード「XYZ」を用いてサービスサイト70のインターネットディスクリソース71のファイルをアクセスしたり、インターネットグループウェア個人情報71aとインターネットグループウェアグループ情報71eをアクセスすることにより、山田氏は、社外にいても社内でアクセスするマスターデータと同一の内容の複製データをアクセスできる。

【0054】また、この実施の形態によれば、一つのシ

システム制御装置で各メンバーがアクセスするグループウェアの情報とファイルとの管理を同時にできるとともに、プロパティ付加部により複製データにプロパティが付加されているので、過去のファイル情報や他の環境から操作したファイルの情報をバックデートして参照することができる。

【００５５】また、この実施の形態によれば、マスターデータは全てイントラネット上に保全され、また、データの転送は、全てイントラネットのシステム制御装置から又はクライアントから又はアクセス端末から行われることにより、データの移動動作の負荷は分散され、サービスサイトのサーバに集中することがなく、本来の業務のレスポンス低下を防ぐことができ、更に、複数のシステム制御装置をサービスサイト経由で連携させて動作させることができるので、システムの規模に応じたスケールビリティを確保することができる。

【００５６】また、この実施の形態によれば、各ファイルをイントラネットあるいはインターネット上のディスクリソースに重複して分散配置し、なおかつ、マスターファイルは、イントラネット上にあるので、ファイルの保全性を高められると同時に、社外のネットワーク障害等に対する耐障害性を確保することができる。

【００５７】実施の形態２、実施の形態１では、サービスサイト７０にＡ社のマスターデータの複製データを常時置くことになっているが、サービスサイト７０には複製データを常時置かずに、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータをアクセスできるようにしてもよい。サービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータをアクセスする場合は、複製データはサービスサイト７０に滞留しない。即ち、上記サービスサイト７０に記憶されるファイルは、ディスク上の一時ファイル、又は、メモリ上のキャッシュファイルで良い。上記サービスサイト７０に記憶されるファイルは、一時的な（瞬時的な）ものなので、この方式は、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータを透過アクセスできることを意味する。

【００５８】この場合は、複製データはサービスサイト７０に滞留しない（サービスサイト７０を透過する）ので社外にデータ保持されず、ユーザのクリティカルなデータが企業内のファイルサーバのみに集中管理され、セキュリティの向上が図れる。以下、ディスク上の一時ファイルを用いて、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータを透過的にアクセスする場合について説明する。

【００５９】１．Ａ社ネットワーク１００のシステム制御装置６０はサービスサイト７０に対してコネクション

を確立して（或いは、ポーリングをして）、Ａ社ネットワーク１００の外部からのアクセスに備える。

２．携帯端末８０又は携帯電話９０はサービスサイト７０に対してデータの転送を要求する。

３．データの転送要求を受信したサービスサイト７０は、システム制御装置６０に対して、携帯端末８０又は携帯電話９０からのデータの転送要求の内容を伝える。

４．携帯端末８０又は携帯電話９０からのデータの転送要求の内容に基づき、システム制御装置６０は、マスターデータのなかから要求されたデータのみをサービスサイト７０に対して転送する。

５．上記サービスサイト７０のインターネットディスクリソース７１は、システム制御装置６０から転送されたデータを受け取り、受け取ったデータをディスク上の一時ファイルとして記憶する。

６．携帯端末８０又は携帯電話９０は、サービスサイト７０のインターネットディスクリソース７１にディスク上の一時ファイルとして一時的に記憶されたデータを自分に転送する。

７．携帯端末８０又は携帯電話９０での転送が完了した時点でサービスサイト７０は、インターネットディスクリソース７１のディスク上の一時ファイルを消去する。

【００６０】次に、キャッシュファイルを用いて、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータを透過的にアクセスする場合について説明する。

１．サービスサイト７０には、インターネットディスクリソース７１の代わりに（或いは、インターネットディスクリソース７１とともに）、サービスサイト７０の外部からのアクセスを高速にする目的でキャッシュメモリ（図示せず）を予め置く。

２．携帯端末８０又は携帯電話９０はサービスサイト７０に対してデータの転送を要求する。

３．データの転送要求を受信したサービスサイト７０は、携帯端末８０又は携帯電話９０が転送要求しているデータファイルがキャッシュメモリに有るか否かをチェックし、そのデータファイルがキャッシュメモリに有れば、そのデータファイルをキャッシュメモリから取得して携帯端末８０又は携帯電話９０に送信する。そのデータファイルがキャッシュメモリにない場合は、サービスサイト７０は、システム制御装置６０に対して、携帯端末８０又は携帯電話９０からのデータの転送要求の内容を伝える。

４．携帯端末８０又は携帯電話９０からのデータの転送要求の内容に基づき、システム制御装置６０は、要求されたデータをサービスサイト７０に対して転送する。

５．上記サービスサイト７０のインターネットディスクリソース７１は、システム制御装置６０から転送されたデータを受け取り、受け取ったデータをキャッシュファ

イルとして記憶する。すでにキャッシュメモリが他のデータファイルで占有されており空き領域がない場合には、LRU (least recently used) 等の公知のアルゴリズムを用いてキャッシュメモリのデータファイルの内容が新たなデータファイルの内容で上書きされる。

6. 携帯端末80又は携帯電話90は、サービスサイト70のキャッシュファイルとして一時的に記憶されたデータを自分に転送する。

【0061】以上のようなシステムでは、膨大なディスクリソース等を持ち保守するリスクは発生しない。即ち、複製データを一時ファイル、又は、キャッシュファイルにして、複製データを消すようにしたので、大容量の記憶装置がいらなくなる。

【0062】ここで、システム制御装置60をA社、B社等のユーザに販売し、さらに、サービスサイト70を運営して、毎月A社、B社等のユーザから、サービスサイト70への接続料を徴収している会社を、以下、「サービス提供者」と呼ぶことにする。上記システムを、「サービス提供者」の立場からみた場合、A社、B社等のユーザは、インターネット上のサービスサイト70をゲートウェイとしてアクセスするので、A社、B社等のユーザの各部門、各支店、各工場の各インターネット接続をサービスサイト70に束ねることができる。上記システムでは、A社、B社等の各ユーザの社員は、社外、各部門、各支店、各工場において自分の社内にある情報をアクセスする場合、携帯端末80又は携帯電話90を用いて、サービス提供者のサービスサイト70に一旦接続することにより、自分の社内にある情報を自由にアクセスすることができる。社外、各部門、各支店、各工場にいる社員は、社内のデータをアクセスするために、サービス提供者のサービスサイト70に接続しないといけないので、サービス提供者は、サービスサイト70を経由して、ユーザに対して、情報検索、情報整理、情報提供等の新しいビジネスモデルを提供することができる。例えば、サービス提供者は、サービスサイト70から、ユーザの社員にお知らせを一齐同報したり、ユーザの社内情報を一括して吸い上げたりというサービスを各ユーザごとに提供することができるようになる。

【0063】また、例えば、A社のX工場でシステム制御装置60が採用されて実施の形態1又は2で述べたシステムがA社のX工場に所属する社員に適用され、次に、A社のY工場でシステム制御装置60が採用されて実施の形態1又は2で述べたシステムがA社のY工場に所属する社員に適用され、さらに、A社の本社でシステム制御装置60が採用されて実施の形態1又は2で述べたシステムがA社の本社に所属する社員に適用されるといように、順次このシステムが使われるようになった後、サービスサイト70にA社がA社ポータルサイトを作れば全社ポータルサイトが完成する。このように、最

初は、会社の一部の組織で利用されていたシステムが最後は会社全体で利用されるようになり、サービス提供者は、会社の一部の組織から会社全体を相手にビジネスができるようになる。

【0064】実施の形態3. 前述した実施の形態1, 2では、転送する内容は主にデータ(例えば、ファイルされたデータ又はスケジュールデータ)であるが、転送する内容を、データそのものではなく、入出力(インプットアウトプット: IO)コマンド、例えば、SCSI (スモールコンピュータシステムインタフェース)でアクセスされるディスク装置に対するリードコマンド及びライトコマンドにしてもよい。

【0065】例えば、携帯端末80がシステム制御装置60のイントラネットディスクリソース61に対して“ファイル”を送るのではなく、イントラネットディスクリソース61のディスクIOコマンドを直接送るようにする。

【0066】ここで用いられるディスクIOコマンドは、例えば、ディスク装置をブロックアクセスデバイスとしてアクセスするコマンドである。携帯端末80が転送するディスクIOコマンド(ディスクリードコマンド又はディスクライトコマンド)は、システム制御装置60で動作しているOS(オペレーティングシステム)がイントラネットディスクリソース61をリード・ライトするときのコマンドと同じもの(同じコマンドフォーマットでかつ同じパラメータ)でなければいけない。イントラネットディスクリソース61がSCSIを用いて接続されている場合には、一般的には公知のSCSIコマンドをそのまま使用することができる。

【0067】ディスクIOコマンドを直接送る手順はデータの転送の場合と同様である。一例として、以下に、携帯端末80がシステム制御装置60のイントラネットディスクリソース61に対してディスクリードコマンドを直接送ってマスクデータを読み取る手順を説明する。

- 【0068】1. システム制御装置60がサービスサイト70に対してコネクションを確立する。
2. 携帯端末80はサービスサイト70に対してディスクリードコマンドの転送要求を出す。
3. サービスサイト70は、携帯端末80からディスクリードコマンドを受信し、システム制御装置60に転送する。
4. システム制御装置60はサービスサイト70からディスクリードコマンドを受け取り、イントラネットディスクリソース61に対してディスクリードコマンドを実行する。
5. システム制御装置60は、リードしたデータをサービスサイト70に対して転送する。
6. サービスサイト70はデータをさらに要求もとの携帯端末80に対して送る。

以上がディスクリードコマンドの転送によるリード処理

の手順である。

【0069】次に、携帯端末80からディスクライトコマンドを用いてシステム制御装置60のイントラネットディスクリソース61にデータを書き込む場合の手順を以下に説明する。

【0070】1．システム制御装置60がサービスサイト70に対してコネクションを確立する。  
2．携帯端末80はサービスサイト70に対してディスクライトコマンドと書き込みデータとが発生したことを通知する。  
3．サービスサイト70は、携帯端末80からの通知を受信し、システム制御装置60に転送する。  
4．システム制御装置60は、サービスサイト70から通知を受け取り、ディスクライトコマンドと書き込みデータとが携帯端末80に有ることを知る。  
5．システム制御装置60は、ディスクライトコマンドと書き込みデータとをサービスサイト70経由で（或いはインターネット10経由で）能動的に携帯端末80に取得しに行く。

6．システム制御装置60は、取得したディスクライトコマンドと書き込みデータとを用いて書き込み処理を実行する。  
以上がディスクライトコマンドの転送によるライト処理の手順である。

【0071】以上のように、サービスサイト70は、携帯端末80が生成したマスタデータに対する入出力コマンドをシステム制御装置60に対して転送する。また、システム制御装置60は、サービスサイト70から転送された入出力コマンドをマスタデータに対して実行する。したがって、携帯端末80からシステム制御装置60に対してデータの読み書きを指示することができ、データそのものを転送する場合に比べて、より柔軟性のあるシステムとなる。

#### 【図面の簡単な説明】

【図1】 本発明の全体システムの一実施の形態を示すブロック図である。

【図2】 図1におけるイントラネットでのユーザインタフェースの関係を示すブロック図である。

【図3】 図1におけるインターネットでのユーザインタフェースの関係を示すブロック図である。

【図4】 図1におけるグループウェア情報管理部の処理動作を示すブロック図である。

【図5】 図4におけるデータブロックのフォーマットを示す図である。

【図6】 図1におけるディスクリソース上のデータの配置を示すブロック図である。

【図7】 図6におけるデータブロックの処理を示すブロック図である。

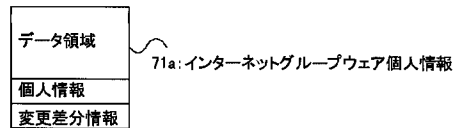
【図8】 図1におけるファイル情報管理部に係るデータの操作を示すブロック図である。

【図9】 従来のシステムを示すブロック図である。

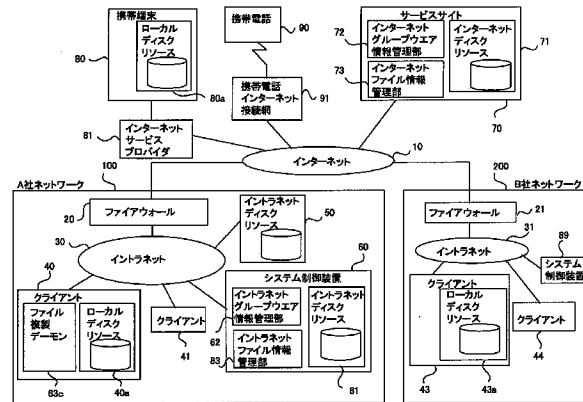
#### 【符号の説明】

10 インターネット、20 ファイアウォール、21 ファイアウォール、30 A社イントラネット、31 B社イントラネット、40 クライアント、41-44 クライアント、60 システム制御装置、61 イントラネットディスクリソース、62 イントラネットグループウェア情報管理部、63 イントラネットファイル情報管理部、70 サービスサイト、71 インターネットディスクリソース、72 インターネットグループウェア情報管理部、73 インターネットファイル情報管理部、80 携帯端末、81 インターネットサービスプロバイダ、90 携帯電話、91 携帯電話インターネット接続網、100 A社ネットワーク、200 B社ネットワーク。

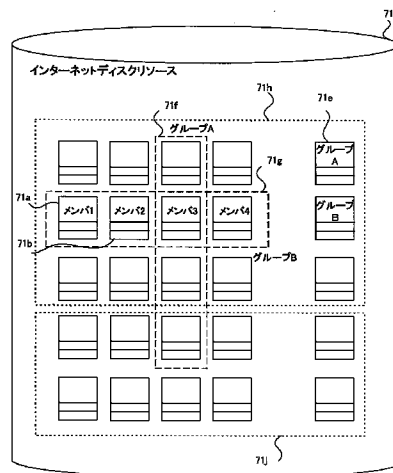
【図5】



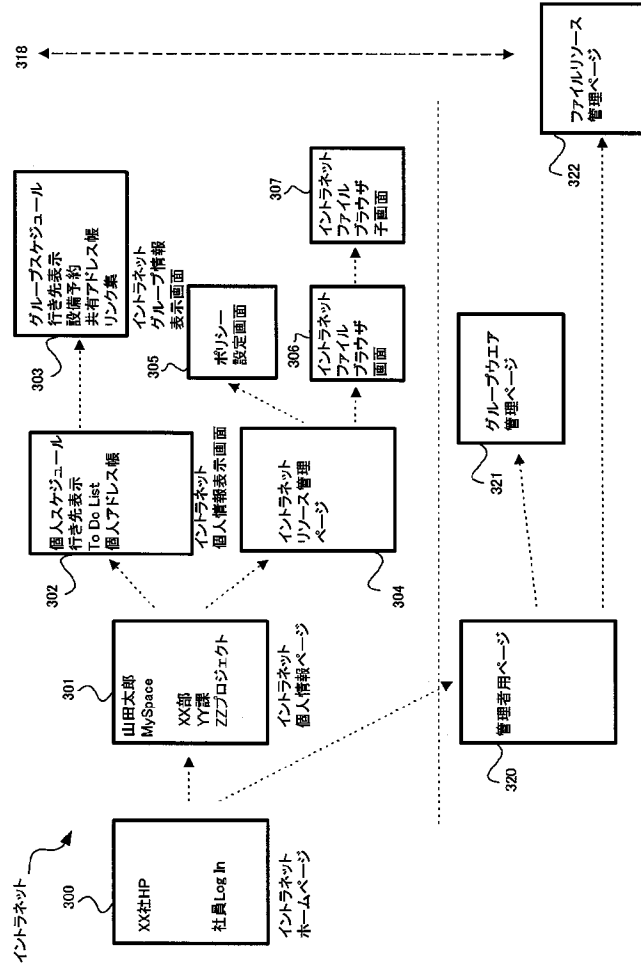
【図1】



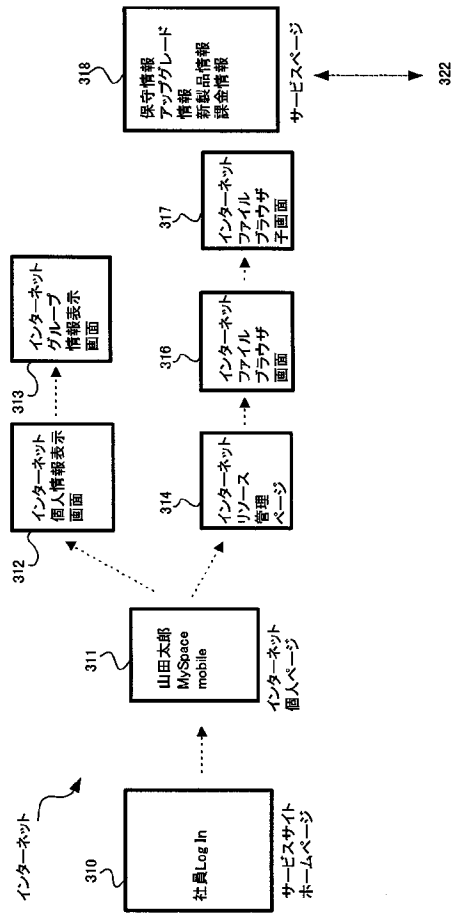
【図6】



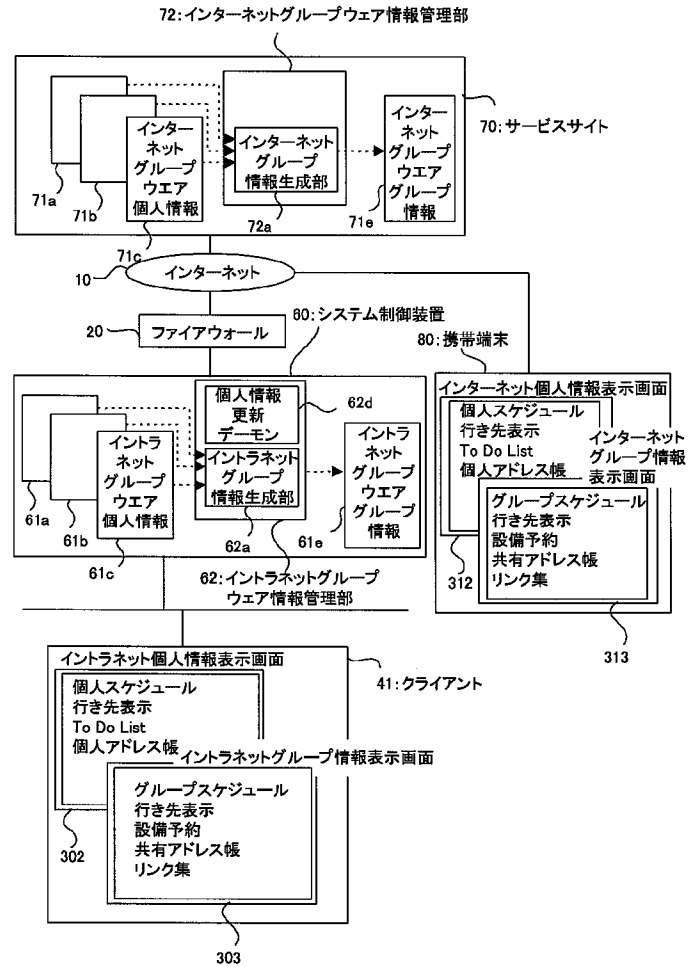
【図2】



【図3】

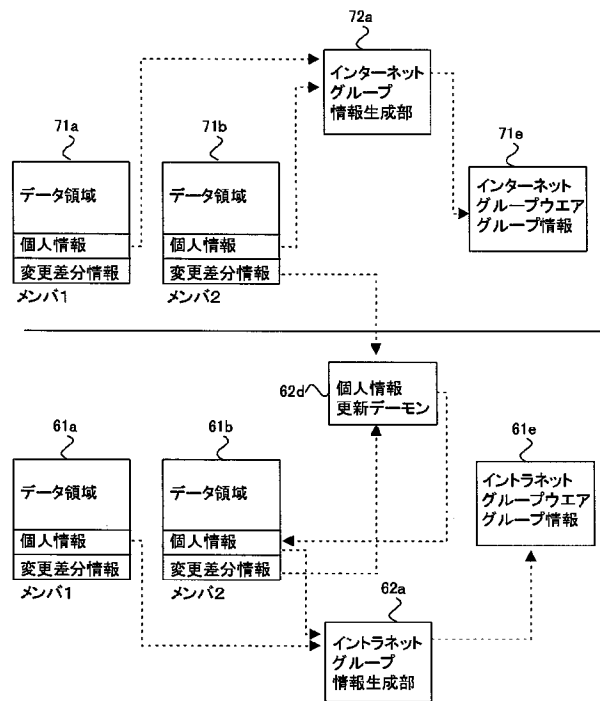


【図4】



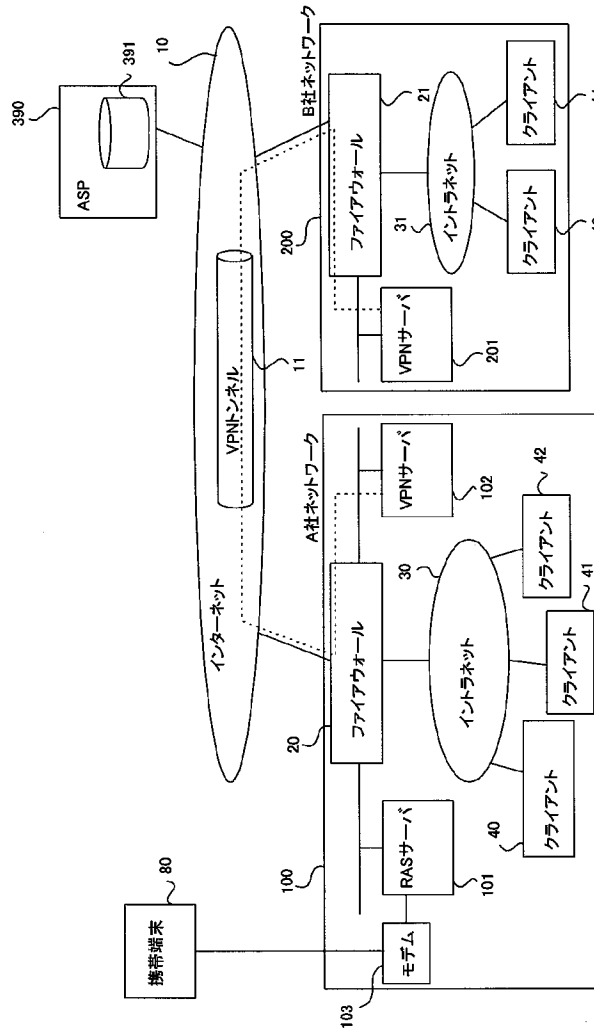


【図 7】





【図9】



( 19 ) 102-140239 ( P2002- ' 39

フロントページの続き

F ターム( 参考 ) 5B082 GB02 GB06 HA03  
5B085 AA01 AE00  
5B089 GA11 JA40 KA17 KB13